IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
ASHEVILLE DIVISION

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH GOOGLE ACCOUNTS: ANDREWDEVINNEY94@GMAIL.COM AND SSTAME324@GMAIL.COM, THAT ARE STORED AT PREMISES CONTROLLED BY GOOGLE AT 1600 AMPHITHEATRE PARKWAY, MOUNTAIN VIEW, CA 94043	Case No. 1:25-mj-3 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Jared Schaefer, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain Google accounts that are stored at premises owned, maintained, controlled, or operated by Google LLC ("Google"), an electronic communications service and/or remote computing service provider headquartered at 1600 Amphitheater Parkway, Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This Affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Google disclose to the government records and other information in its possession, pertaining to the subscriber(s) or customer(s) associated with the accounts.

2. I am a Special Agent with the Federal Bureau of Investigation Charlotte Division / Hickory Resident Agency and have been since October 2023. My career in law enforcement began in May 2020, where I spent three years as a sworn Police Officer/Detective with the La Porte Police Department (LPPD) in Indiana. I spent approximately the first year tasked with completing

the police academy, performing road patrol duties which consisted of responding to 911 calls for police assistance for all types of crimes, conducting self-initiated activities to deter crime, taking part in community engagement initiatives and numerous other jobs vital to LPPD's mission; being a member of the Detective Bureau where I conducted a number of logical investigations into robberies, burglaries, sexual assaults, child molestations, murder, and other violent crimes for approximately two years. In my time as a law enforcement officer, I have received several hundred hours of training in the investigations of general crimes, and I have been directly or indirectly involved with investigations of cases of child sexual assault. I have participated in the execution of numerous search warrants, which have resulted in the seizure of evidence and the successful prosecution of individuals.

3. For the purpose of supporting this Application for a Search Warrant, I have set forth herein facts that I believe are sufficient to establish probable cause to believe that evidence of violations of 18 U.S.C. § 2252A(a)(2)(A) (receipt and distribution of child pornography), and 18 U.S.C. § 2252A(a)(5)(B) (possession of, knowing access, or attempted access with intent to view child pornography) by Andrew C. DEVINNEY and Starla STAMEY will be found in the Google account(s) described below:

a. andrewdevinney94@gmail.com
b. sstame324@gmail.com

4. This Affidavit refers to the above Google accounts collectively as the "TARGET ACCOUNTS." The TARGET ACCOUNTS are further described in Attachment A. The TARGET ACCOUNTS are stored at premises owned, maintained, controlled, or operated by Google. The applied-for warrant would order Google to provide information described in Attachment B.

5. The information in this Affidavit is based upon my personal knowledge, training, and experience, and the information learned, either directly or indirectly, from witnesses, records, and other law enforcement officers and agents. This Affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

PROBABLE CAUSE

6. On August 5, 2024, the Burke County Sheriff's Office (BCSO) received three CyberTips from the National Center for Missing and Exploited Children (NCMEC) regarding the distribution and receipt of child pornography between Andrew C. DEVINNEY and Starla STAMEY. Two of the three CyberTips documented distributions of child pornography via Facebook Messenger. The third CyberTip documented distributions of child pornography between DEVINNEY and STAMEY via Snapchat. NCMEC's CyberTipline reporting system allows electronic service providers, like Facebook and Snapchat, to make reports of suspected online sexual exploitation of children, including the distribution and receipt of child pornography, occurring on their platforms.[1]

CyberTip 1

6. NCMEC received CyberTip #194669154 (CyberTip 1) from Facebook on June 4, 2024, at approximately 10:20PM (UTC). This tip identified DEVINNEY as sending files depicting child pornography to STAMEY via Facebook Messenger.

[1] "Overview," National Center for Missing & Exploited Children CyberTipline, https://www.missingkids.org/gethelpnow/cybertipline.

7. CyberTip 1 identified a total of three files that DEVINNEY sent to STAMEY on May 30, 2024, at approximately 2:09PM (UTC), using Facebook Messenger username "Andrew DeVinney" (screenname: andrew.devinney.3). Facebook identified one of the three files sent by DEVINNEY as depicting child pornography by running the file's unique MD5 hash value[2] against hash values for known series of child pornography and confirmed that the file did in fact match a previously identified video of child pornography. The identified file depicted a one minute and fifty-four second video of an adult white male forcing vaginal sex on a 6- to 8-year-old prepubescent female.

8. According to Facebook records, the "Andrew DeVinney" Facebook account was associated with phone numbers 828-302-9582 and 828-403-4141. The email address associated with the "Andrew DeVinney" Facebook account was andrewdevinney94@gmail.com. DEVINNEY's Facebook account used IP address 75.143.188.107, which was provided by Spectrum/Charter to a location in Morganton, North Carolina.

9. According to Facebook records, STAMEY's Facebook Messenger account used the screen name "Starla.stamey.3" and was associated with phone number 828-409-4061. CyberTip 1 reported that STAMEY's birth date was July 23, 1995, and that STAMEY's account was used in Morganton, North Carolina. STAMEY's listed verified phone number was 828-409-

[2] A hash value is a unique numeric value that is assigned to a digital file by processing it through a cryptographic algorithm. MD5 is a commonly used cryptographic algorithm to generate hash values. This number, the hash value, becomes a unique identifier for the file. Any change to the digital file likewise will change the hash value. Hash values are often analogized to a DNA profile. The probability of two different digital files sharing the same hash value is nearly impossible, so if two files have the same hash value then one may safely assume that the files are identical.

4061. The IP address listed for STAMEY's account was 149.168.240.6, which resolved to a Virtual Private Network (VPN)[3] server in the Raleigh, North Carolina area.

10. NCMEC performed a public records search of the phone numbers from CyberTip 1. Phone number 828-403-4141 belongs to an AT&T Mobility account held by DEVINNEY at 3695 Ridge Ct., Morganton, North Carolina 28655. Phone number 828-302-9582 belongs to a T-Mobile account held by STAMEY, also at 3695 Ridge Ct., Morganton, North Carolina 28655.

CyberTip 2

11. NCMEC received CyberTip #195424149 (CyberTip 2) from Facebook on June 20, 2024, at approximately 4:30PM (UTC). This tip also identified DEVINNEY as sending child pornography to STAMEY via Facebook Messenger.

12. CyberTip 2 identified ten files that DEVINNEY sent to STAMEY on June 17, 2024, at approximately 4:21PM (UTC), two of which depicted child pornography.

13. CyberTip 2 provided all the same account information regarding the Facebook Messenger accounts for DEVINNEY and STAMEY that were provided in CyberTip 1, including the telephone numbers.

14. The two files identified as child pornography in CybterTip 2 depicted the following:

a. A video lasting approximately 30 seconds of a pubescent white female, approximately 12-14 years old, masturbating.

[3] Your Affiant knows that a VPN is a computer-based service that encrypts data and masks IP addresses to create a secure connection between a device and a remote server. A VPN user may be connected to a server in Raleigh, North Carolina without being in the vicinity of Raleigh.

b. A video lasting approximately 44 seconds of a prepubescent white female, approximately 10-12 years old, exposing her vagina and breasts.

CyberTip 3

15. NCMEC CyberTip #194482571 (CyberTip 3) was received by NCMEC from Snapchat on May 31, 2024, at approximately 6:17PM (EST). CyberTip 3 documented a file named in part "devinney1617" being uploaded to the Snapchat social media application on May 30, 2024, at approximately 10:15AM, by Snapchat account username devinney1617. CyberTip 3 identified this file as depicting child pornography based on a review by an individual at Snapchat.

16. CyberTip 3 further detailed that the "devinney1617" file was uploaded by a Snapchat account associated with phone number (828) 302-9582 and the email address andrewdevinney94@gmail.com. The IP address that the file was uploaded from was 75.143.188.107. The date of birth associated with the Snapchat account user was February 27, 1994.

Agents identify and interview DEVINNEY and STAMEY

15. The North Carolina State Bureau of Investigation (NCSBI) served an administrative subpoena on Charter Communications for account information associated with IP address 75.143.188.107 in service on May 30, 2024, at approximately 10:58AM (UTC). Charter Communications responded with the following account information:

Subscriber Name: Andrew DeVinney
Service Address: 3695 Ridge Ct. Morganton, NC 28655-9170
User Name or Features: andrew_devinney@charter.net, andrewdevinney@charter.net, andrewdevinney0811@charter.net, andrewdevinney94@gmail.com, and doofy_marine@charter.net.
Account Number: 8315202290391189

MAC: 2CEADCB11273
Lease Log: Start Date: 07/01/2022 8:53PM / End Date: 07/20/2024 1:27PM

16. FBI agents located and interviewed DEVINNEY on August 13, 2024. During his interview, DEVINNEY explained that he and STAMEY reside with one another, have two children together, and are engaged. DEVINNEY confirmed his and STAMEY's Facebook account information and admitted to sending large amounts of pornography to STAMEY but claimed to be unsure whether he ever sent her child pornography. DEVINNEY also disclosed an old Facebook account under the name of "John Smith" that he claimed not to use anymore.

17. An FBI agent and a BCSO detective located and interviewed STAMEY on August 26, 2024. STAMEY admitted that DEVINNEY began sending her child pornography approximately a year prior. DEVINNEY transmitted almost all the child pornography material via Facebook Messenger. STAMEY also admitted to using Reddit and Google to download child pornography and send it to DEVINNEY via Facebook Messenger. STAMEY disclosed that DEVINNEY downloaded most of the child pornography from Kik and Reddit before sending it to her on Facebook Messenger. STAMEY was unsure of the quantity of child pornography that she and DEVINNEY traded but affirmed that they had shared a large amount. STAMEY's iPhone 13 Pro Max was seized during search warrant execution at their residence on August 13, 2024, and forensically extracted as well.

Discovery of the TARGET ACCOUNTS

18. FBI agents seized DEVINNEY's Samsung S24 cell phone during his interview. Pursuant to a Federal search warrant, FBI performed a forensic analysis of DEVINNEY's cell phone and confirmed that it used the phone number 828-302-9582. Agents also recovered images depicting child pornography from the device. The forensic analysis revealed that DEVINNEY

began using his cell phone to download and view child pornography at least as early as September 20, 2019, and confirmed that DEVINNEY used the cell phone to send child pornography to STAMEY on July 12, July 29, and August 12, 2024. Agents also discovered that DEVINNEY had used his cellphone to send child pornography to his "John Smith" Facebook account on July 12, 2024.

The andrewdevinney94@gmail.com Google Account

19. DEVINNEY's Samsung S24 was determined to be his primary mobile device. The primary user account associated with that device is andrewdevinney94@gmail.com.

20. A review of the backup history of DEVINNEY's cellphone showed that he regularly backed up the content of his phone to his andrewdevinney94@gmail.com Google Account. Among other things on his cellphone, these backups included images and videos of child pornography created by DEVINNEY as well as other files depicting child pornography that appear to have been downloaded from the Internet. A surreptitious video of MFV1 taking a shower was backed up to this email.

21. FBI agents were also able to see from DEVINNEY's cellphone that DEVINNEY regularly used the cloud storage service made available by Google through his andrewdevinney94@gmail.com account.

22. During the forensic analysis of DEVINNEY's Samsung S24, it was discovered that DEVINNEY used his cell phone to secretly film a nine-year-old female (Minor Female Victim 1, or MFV1) taking a shower while at DEVINNEY's home on at least on two occasions. One such video shows DEVINNEY setting up his phone in a surreptitious location in a bathroom. After DEVINNEY set the Samsung S24 at the angle he desired, he is seen getting the shower set up for MFV1. MFV1 entered the bathroom where they converse for a few moments.

MFV1 watched DEVINNEY leave the bathroom before undressing herself. MFV1 is seen taking a shower for several minutes. Once MFV1 is done and dressed, she exits the bathroom where DEVINNEY's daughter then enters to shower. The video captured her showering as well, but DEVINNEY comes in shortly after she enters and stops the recording.

23. DEVINNEY also used his Samsung S2 to photograph himself masturbating to this content. The images that DEVINNEY created of himself show DEVINNEY masturbating to still images and videos of MFV1. It was apparent from the Samsung S24 that these files had been viewed, accessed, and/or stored with the following sources on the phone:

a. Remotely viewed directly from the andrewdevinney94@gmail.com Google Photos account.

b. Stored locally in the phone's directories under andrewdevinney94@gmail.com/localmedia/"File name".

c. Created using the Samsung S24 cellphone and stored in the phone's directory under data/media/0/DCIM/Camera/"File name".

d. Stored in a Google cloud storage account associated with the andrewdevinney94@gmail.com Google account.

24. The forensic review of DEVINNEY's Samsung S24 revealed that DEVINNEY had also been using the social media application Kik to receive child pornography. DEVINNEY used the Kik screenname "tribgod0811_mro@talk.kik.com" to communicate with other Kik users about the sexual exploitation of children and to send and receive child pornography. Legal process sent to Kik by the FBI revealed that DEVINNEY's "tribgod0811_mro@talk.kik.com" account was associated with the Google account, andrewdevinney94@gmail.com.

The sstame324@gmail.com Google account

25. In addition to the Google accounts for andrewdevinney94@gmail.com and andrewdevinney22@gmail.com, a Google account under sstame324@gmail.com was also discovered on DEVINNEY's Samsung S24. The following interactions between the andrewdevinney94@gmail.com and sstame324@gmail.com accounts were found on DEVINNEY's Samsung S24:

a. Child pornography images of MFV1 found on DEVINNEY's cellphone that included meta data showing that the images were created using STAMEY's iPhone 13 Pro Max cellphone.

b. Child pornography images of MFV1 being shared between STAMEY and DEVINNEY's Facebook accounts, including the "John Smith" Facebook account. All three accounts were logged into on DEVINNEY's Samsung S24.

c. Sstame324@gmail.com was the second most accessed account on the Samsung S24 cellphone with over 500 user interactions dating to at least January 2024.

d. Sexual content was transferred between the andrewdevinney94@gmail.com and sstame324@gmail.com accounts.

e. Access to Google Photos cloud-based data for both the sstame324@gmail.com and andrewdevinney94@gmail.com accounts.

26. After performing a forensic review of STAMEY's iPhone 13 Pro Max, it was determined that the sstame324@gmail.com Google account was the primary user account for that device.

27. On November 6, 2024, FBI agents sent preservation requests to Google for the TARGET ACCOUNTS. The TARGET ACCOUNT(S) have been preserved for 90 days.

BACKGROUND CONCERNING GOOGLE[4]

28. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

29. In addition, Google offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

30. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account.

---

[4] The information in this section is based on information published by Google on its public websites, including, but not limited to, the following webpages: the "Google legal policy and products" page available to registered law enforcement at lers.google.com; product pages on support.google.com; or product pages on about.google.com.

31. Google advertises its services as "One Account. All of Google working for you." Once logged into a Google Account, a user can connect to Google's full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

32. Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google. Gmail can be accessed through a web browser or a mobile application. Additional email addresses ("recovery," "secondary," "forwarding," or "alternate" email addresses) can be associated with the Google Account by the user. Google preserves emails associated with a Google Account indefinitely, unless the user deletes them. Google also provides an address book for Google Accounts through Google Contacts. Google Contacts stores contacts the user affirmatively adds to the address book, as well as contacts the user has interacted with in Google products. Google Contacts can store up to 25,000 contacts. Users can send messages to more than one contact at a time by manually creating a group within Google Contacts or communicate with an email distribution list called a Google Group. Users have the option to sync their Android mobile phone or device address book with their account so it is stored in Google Contacts. Google preserves contacts indefinitely, unless the user deletes them. Contacts can be accessed from the same browser window as other Google products like Gmail and Calendar.

33. Google provides several messaging services including Duo, Messages, Hangouts, Meet, and Chat. These services enable real-time text, voice, and/or video communications through browsers and mobile applications, and also allow users to send and receive text messages, videos, photos, locations, links, and contacts. Google may retain a user's messages if

the user hasn't disabled that feature or deleted the messages, though other factors may also impact retention. Google does not retain Duo voice calls, though it may retain video or voicemail messages.

34. Google Drive is a cloud storage service automatically created for each Google Account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can set up their personal computer or mobile phone to automatically back up files to their Google Drive Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called "Shared with me." Google preserves files stored in Google Drive indefinitely, unless the user deletes them. Google Keep is a cloud-based notetaking service that lets users take notes and share them with other Google users to view, edit, or comment. Google Keep notes are stored indefinitely, unless the user deletes them.

35. Google integrates its various services to make it easier for Google Accounts to access the full Google suite of services. For example, users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout, Meet, and Chat

conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

36. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

37. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

38. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

39. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

40. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation.

41. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).

42. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, the apps downloaded from the Google Play store may reveal services used in furtherance of the crimes under investigation or services used to

communicate with co-conspirators. In addition, emails, instant messages, Internet activity, and documents can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

43. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

15. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

44. Based on the forgoing, I request that the Court issue the proposed search warrant.

45. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

This search warrant affidavit has been reviewed by AUSA Alexis Solheim.

Respectfully,

/s/ Jared Schaefer
Jared Schaefer
Special Agent FBI

In accordance with Rule 4.1(b)(2)(A), the Affiant attested under oath to the contents of this Affidavit, which was submitted to me by reliable electronic means, on this 29th day of January, 2025, at 9:13 AM

W. Carleton Metcalf
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the following Google accounts (TARGET ACCOUNTS) that are stored at premises owned, maintained, controlled, or operated by Google LLC., a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043:

- andrewdevinney94@gmail.com
- sstame324@gmail.com

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC.

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, text messages, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on November 6th, 2024, with the Google Reference Number 74023008, Google is required to disclose to the government for the accounts and identifiers listed in Attachment A (the TARGET ACCOUNTS) the following information:

1. All business records and subscriber information, in any form kept, pertaining to the TARGET ACCOUNTS, including:

   a. Names (including subscriber names, user names, and screen names);

   b. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);

   c. Telephone numbers, including SMS recovery and alternate sign-in numbers;

   d. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions, including log-in IP addresses;

   e. Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address, SMS recovery numbers, Google Voice numbers, and alternate sign-in numbers;

f. Length of service (including start date and creation IP) and types of service utilized; and

g. Change history.

2. All device information associated with the TARGET ACCOUNTS, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;

a. Records of user activity for each connection made to or from the Account(s), including, for all Google services, the date, time, length, and method of connection, data transfer volume, user names, source and destination IP address, name of accessed Google service, and all activity logs;

b. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the size, length, and timestamp of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails;

c. Any records pertaining to the user's contacts, including: address books; contact lists; social network links; groups, including Google Groups to which the user belongs or communicates with; user settings; and all associated logs and change history;

d. The contents of all text, audio, and video messages associated with the account, including Chat, Duo, Hangouts, Meet, and Messages (including SMS, MMS, and

RCS), in any format and however initially transmitted, including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size, length, and timestamp of each communication; user settings; and all associated logs, including access logs and change history;

e. All photo and videos associated with and contained in the account, including all photos and videos contained in the Google Photos service and/or application, as well as all photos and videos attached to emails and/or any other communications contained in or associated with the account;

f. All Internet search and browsing history, and application usage history, including Web & App Activity, Voice & Audio History, Google Assistant, and Google Home, including: search queries and clicks, including transcribed or recorded voice queries and Google Assistant responses; browsing history, including application usage; bookmarks; passwords; autofill information; alerts, subscriptions, and other automated searches, including associated notifications and creation dates; user settings; and all associated logs and change history.

Google is hereby ordered to disclose the above information to the government within 7 days of issuance of this warrant.

II. Information to be seized by the government

1. All information described above in Section I, including correspondence, records, documents, photos, videos, electronic mail, chat logs, and other electronic text messages, that constitute fruits, evidence, and instrumentalities of the crimes under investigation, that is, violations of 18 U.S.C. §§ 2251(a) and 2252(a)

(production, attempted production, distribution, and possession of child pornography) including, for the TARGET ACCOUNTS listed on Attachment A, information pertaining to the following matters:

a. Any and all communications, dated from July 1, 2023 through August 13, 2024, whether by email, text message, or voicemail, and including any attached media (photos and videos), between the TARGET ACCOUNTS users Andrew DEVINNEY and Starla STAMEY evidencing the relationships between and among these individuals, including those referring to or concerning the sexual exploitation of any minor and/or any investigation by law enforcement or child social service agency of such conduct;

b. Any and all records, information, and communications, dated from July 1, 2023 through August 13, 2024, in any form, including all temporary and permanent electronic files and records, (including, but not limited to, JPG, GIF, TIF, AVI, WAV and MPEG files) which contain, attach, or describe visual depictions of minors;

c. Any and all records, information, and communications, dated from July 1, 2023 through August 13, 2024, in any form, pertaining to the sexual exploitation of minors;

d. Any and all records, information, and communications, dated from July 1, 2023 through August 13, 2024, about any and all internet protocol (IP) addresses used by or accessed by the user of the TARGET ACCOUNTS during this time period;

e. Any and all photos and videos depicting minors engaging in sexually explicit conduct as defined in 18 U.S.C. § 2256;

f. Any and all photos and videos that depict MFV1 or MFV2

g. Any and all photos and videos depicting Andrew DEVINNEY and Starla STAMEY

h. Any and all telephone numbers associated with the TARGET ACCOUNTS;

i. Any and all records, information, and communications, dated from July 1, 2023 through August 13, 2024, evidencing how and when the Account was created, accessed, and used, to determine the geographic location(s) and chronological context of the crimes under investigation;

j. Any and all records, information, photos, recordings, and communications that reference or reflect the identity of (i) the person(s) who created, used, owned, and/or controlled the Account, and (ii) the person(s) who used, owned and/or controlled any mobile device or computer that accessed or was linked to the TARGET ACCOUNTS; and

2. Passwords and encryption keys, and other access information that may be necessary to access the TARGET ACCOUNTS listed in Attachment A.

This search warrant shall include authority to analyze and search any of the aforementioned items for relevant evidence via submission to the appropriate laboratory for examination by a forensic examiner.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and

instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete or partial copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by [[**CHOOSE APPLICABLE:** Google LLC **AND/OR** Google Payment Corporation]] ("Google"), and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, and they were made by Google as a regular practice; and

b. such records were generated by Google's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature